Department of Homeland Security Daily Open Source Infrastructure Report for 12 January 2009

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- Water Technology Online reports that the mayor of Tacoma, Washington, has declared a civil emergency for the city of about 200,000 due to the threat the rising Puyallup River poses to the city's wastewater treatment plant. (See item **16**)
- According to WebMD, Quest Diagnostics, a company that performs lab tests for patients nationwide, says some of the vitamin D tests it conducted in 2007 and part of 2008 yielded incorrect results. (See item **20**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *January 9, Bloomberg* – (International) **Saudi oil supertanker released by Somali pirates, AFP Reports.** The Saudi Arabian oil supertanker Sirius Star has been released by the Somali pirates who hijacked it in November in the Indian Ocean, Agence France-Presse said, citing the leader of the pirates. "All our people have now left the Sirius Star," AFP cited him as saying January 9 in a phone interview from the pirates' stronghold in the Somali town of Harardhere. "The ship is free, the crew is free." The tanker is in the fleet of Saudi Arabia's state-owned Vela International Ltd. and was carrying 2 million barrels of crude. It was hijacked November 15 about 420 nautical miles off Somalia and was carrying 25 crew members from Britain, Poland, Croatia, and

Saudi Arabia.
Source:
http://www.bloomberg.com/apps/news?pid=20601072&sid=aHnvCuDdwi3A&refer=energy

2. *January 8, Bloomberg* – (National) **Boxer calls for standards on coal ash after Tennessee spill.** At a hearing January 8, a U.S. Senator from California said she would press for regulations on coal ash, after 1 billion gallons of sludge were dumped from a Tennessee Valley Authority (TVA) coal plant December 22. The cost of managing the ash under new standards would be less costly than the pending cleanup, she said. She also said she would look at mandating dry ash, rather than allowing the type of wet sludge that spilled in Tennessee. The TVA chief executive offered no timetable in testimony for cleaning up the December 22 spill that buried 300 acres of eastern Tennessee. Coal ash storage facilities at power plants are not federally regulated and are subject only to state oversight. The industry-funded Utility Solid Waste Activities Group in Washington says that regulating the waste would be costly and unnecessary, while the Washington-based Environmental Integrity Project says that the ash is toxic and can contaminate water supplies. Almost 100 power plants in Florida, Alabama, and at least 10 other states use the same type of coal-ash holding ponds that failed at TVA's Kingston plant on December 22, according to the Environmental Integrity Project, which collected data that companies send to the government.
Source:
http://www.bloomberg.com/apps/news?pid=20601103&sid=aj90MqDXbG.E&refer=us

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

3. *January 8, United Press International* – (National**) X-47B aircraft carrier UAV completes demo.** The follow-on naval variant of Northrop Grumman's X-47 unmanned aerial vehicle has been demonstrated successfully for the U.S. Navy. U.S. companies Northrop Grumman and X-47 engine designer Pratt & Whitney announced the demonstration of the first X-47B UAV as part of the Navy's Unmanned Combat Air System Carrier Demonstration program. The successful demonstration marks a significant milestone for the X-47B, powered by a Pratt & Whitney F100-PW-220U

engine, and also the Navy's initiative to have an aircraft carrier-based advanced UAV technology.
Source: http://www.upi.com/Security_Industry/2009/01/08/X-47B_aircraft_carrier_UAV_completes_demo/UPI-93221231448076/

[Return to top]

Banking and Finance Sector

4. *January 8, Bloomberg* – (New York) **Ponzi scheme targeted Catholics, priests, U.S. says.** U.S. prosecutors and market regulators accused a Buffalo, New York-area investment adviser of operating a Ponzi scheme that targeted Catholics, including priests. The man was charged with mail fraud at federal court in Buffalo, a U.S. attorney said Thursday in a statement. He placed advertisements in Catholic newspapers across the country while raising at least $17 million since 2004, according to the statement. The marketing materials claimed "seniors and clergy are absolutely pleased" with the firm's returns and lack of fees, the Securities and Exchange Commission (SEC) said in a civil lawsuit naming him and his firm, Gen-See Capital Corp. "Investors' funds are not, however, invested in anything," the SEC said. The man told clients their money was invested in "high quality" residential mortgages purchased at a discount, according to the SEC. Instead, funds were misappropriated to pay periodic returns, the regulator said. Payments in November were sent to at least 200 clients, including Catholic priests, religious orders, and cemetery funds, it said. The SEC said it is also seeking an emergency court order freezing the defendants' assets.
Source:
http://www.bloomberg.com/apps/news?pid=20601087&sid=aELIfH1r.knc&refer=home

5. *January 8, Wall Street Journal* – (Pennsylvania) **New Ponzi case pursued.** The Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) brought civil charges against a Pennsylvania man accused of running a $50 million Ponzi scheme since at least February 1995. Authorities said in a complaint Thursday that the man of Broomall, Pennsylvania, turned himself in to authorities in December and signed a confession with the U.S. postal inspector after his alleged Ponzi scheme fell apart. No criminal charges have been filed at this point. According to the SEC, he obtained the $50 million from as many as 80 different investors through the sale of securities in the form of limited partnership interests in his firm, Joseph Forte LP. Authorities claim he told investors he would invest money in an account that trades in securities-futures contracts. The CFTC's complaint, filed in a U.S. District Court in Philadelphia, accuses him of solicitation fraud, misappropriation of commodity-pool funds, sending customers false account statements, and failing to register as a commodity-pool operator. On Wednesday, a U.S. District judge issued an order freezing all of his assets.
Source:
http://online.wsj.com/article/SB123146543612166835.html?mod=googlenews_wsj

6. *January 7, Guardium* – (District of Columbia) **Washington Metropolitan Area Transit Authority implements Guardium to safeguard customer data, automate**

PCI-DSS controls. Guardium, a database security company, announced on January 7 that the Washington Metropolitan Area Transit Authority (Metro) has implemented Guardium's real-time database security and monitoring solution to help safeguard sensitive cardholder data in its heterogeneous, multi-tier database and application environment. With more than 9 million credit and debit card transactions yearly, Metro is classified as a top-tier Level 1 merchant by the Payment Card Industry Data Security Standard (PCI-DSS). The chief of Metro IT Security, Department of Information Technology, Washington Metropolitan Area Transit Authority said, "Guardium has helped us implement robust, hardened 'security zones' around our critical production databases, with a DBMS-independent architecture that doesn't impact performance or require changes to our databases and applications." Guardium is also helping Metro simplify enterprise security by automating and centralizing controls required for compliance. "We initially looked at native DBMS logging and auditing, but it's impractical because of its high overhead, especially when you're capturing every single SELECT (database read operation) in a high-volume environment like ours," he said. "In addition, native auditing doesn't enforce separation of duties or prevent unauthorized access by privileged insiders."
Source: http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=212701129&subSection=Attacks/breaches

[Return to top]

Transportation Sector

7. *January 9, Atlanta Journal-Constitution* – (Georgia) **City searches for causes of why streets collapsed.** Atlanta officials now know what caused part of a downtown Atlanta street to collapse, but the mystery remains about two other collapses in the same area. An Atlanta watershed management spokeswoman said January 8 that three or four large steam vaults recently collapsed under Forsyth Street just south of Alabama Street, causing part of the pavement to give way. The vaults are about 15 feet wide and 14 feet below the street, she said. They probably "date to the '20s, when buildings were heated with steam," she said in an e-mail. The departments of Watershed Management and Public Works began backfilling the vaults with dirt and gravel on January 8, she said. Once that is complete, they will repave the street. Officials still are not sure what caused a Forsyth Street sidewalk to buckle, nor do they know why part of Underground Atlanta's upper plaza collapsed just after midnight on New Year's Day. Engineers were scheduled to visit Underground January 8, but their findings were not immediately known. "It is still under investigation," said a spokeswoman for the city's Public Works Department. All three areas remained cordoned off January 8 evening.
Source: http://www.ajc.com/services/content/metro/stories/2009/01/09/sinkholes.html

8. *January 9, Sun-Times News Group* – (Illinois) **Snowstorm moves into Chicago, more than 150 flights canceled.** A snow storm in the Chicago area snarled traffic and led to flight cancellations Friday morning. The city's Department of Streets & Sanitation deployed 184 snow-fighting trucks to the main roads about 2:30 a.m., according to a department release. The storm has brought traffic on the expressways to a crawl. As of

7:30 a.m. Friday, flight delays at O'Hare were averaging 30 minutes and airlines canceled over 150 flights, according to the Department of Aviation. Midway Airport was reporting minor cancellations and no delays.
Source: http://www.suntimes.com/news/metro/1369594,w-weather-chicago-snow-delays-flights-010908.article

9. *January 8, Columbus Dispatch* – (Ohio) **Travelers say they smelled alcohol, confronted pilot.** The Federal Aviation Administration (FAA) is investigating an incident Tuesday at Port Columbus International Airport in which two passengers accused a Southwest Airlines pilot of having been drinking. Airport police found the captain in a nearby restroom, where he had traded his uniform jacket and cap for a "civilian" jacket, the report said. While in the restroom, the captain apparently called the airline to report that he was sick, triggering his replacement on the Orlando-bound flight. The police officers said the captain did smell of alcohol but did not appear to be impaired. He told them that he had "partied hard" at his hotel the night before but that he had not been drinking that day, the report said. Airline officials told police that the captain would be given a blood-alcohol test. No results were immediately available.
Source: http://www.columbusdispatch.com/live/content/local_news/stories/2009/01/08/PILOT.ART_ART_01-08-09_B3_2ICF6JP.html?sid=101

[Return to top]

Postal and Shipping Sector

10. *January 9, GMANews* – (International) **12 PhilPost employees pass first test for anthrax.** The 12 employees of the Philippine Postal Corp. (PhilPost) who were quarantined on suspicion of anthrax infection tested negative for the disease on first swabbing, the Anti-Terrorism Council (ATC) said Friday. The spokesman for the ATC said the workers would remain quarantined for further tests. PhilPost placed 12 (not 13 as earlier report) of its workers under seclusion after personnel from the U.S. Embassy on Thursday discovered white powder in an envelope in one of the office's incoming mail.
Source: http://www.gmanews.tv/story/143460/12-PhilPost-employees-pass-first-test-for-anthrax

11. *January 8, Chicago Sun-Times* – (Illinois) **White powder in letter sent to Rush's office.** A note containing white powder and "hateful language" was sent to the South Side office of a U.S. Representative on Thursday. Shortly after noon, the Chicago Fire Department was called to the congressman's office, after a white powder was found in a letter sent to the congressman, according to the fire media affairs director. A Level 1 HazMat response was called as a precautionary measure, but the white powder was determined to be a harmless household product, he said. "There is absolutely, positively no threat at all," he said, though adding the letter included "hateful language." A couple of employees in the office opened the letter and alerted authorities. No one was injured, according to the director. Crews were leaving the scene as of 12:45 p.m.
Source: http://www.suntimes.com/news/24-7/1368266,w-letter-white-powder-sent-rush-

office-010809.article

[Return to top]

Agriculture and Food Sector

12. *January 8, USA Today* – (International) **Study warns of dire overheating of crops, food crisis by 2100.** Hotter summers from global warming will drastically reduce crop yields and lead to a disastrous food shortage for billions of people by the end of this century, predicts a study released Thursday in the journal Science. "The hottest seasons on record will represent the future norm in many locations," says the study by a University of Washington atmospheric scientist and the director of Stanford University's program on food security and the environment. While much attention has focused on the threat of increased drought because of climate change, the potential impact of increased temperatures on crops is often overlooked, the report says. In the tropics, higher temperatures — as much as 9 degrees above current summer averages — could cut crop yields by 20 percent to 40 percent, the study says. The crop crisis would not be limited to the tropics. Parts of the United States by 2100 could have typical summers warmer than the highest temperatures recorded from 1900-2006 — along the Eastern Seaboard, the Southeast, the western Plains, the Rockies, and California. "The reality would be somewhat less grim than what they're presenting," because crops would be adapted for higher temperatures, says a researcher with the National Center for Atmospheric Research, in Boulder, Colorado, who was not involved in the report. The director of Stanford University's program on food security and the environment agrees, but notes: "It will take decades to develop new food crop varieties that can better withstand a warmer climate."
Source: http://www.usatoday.com/weather/climate/globalwarming/2009-01-08-climatechange_N.htm

13. *January 8, NewsInferno.com* – (National) **More U.S. infant formula tainted with melamine.** Melamine and its byproduct, cyanuric acid, has been found in more U.S. baby formula, the Food & Drug Administration (FDA) has announced. This is the second time that the industrial chemical has turned up in baby formula in this country, but the FDA continues to insist that U.S. supplies are safe. Melamine is a renal toxin that can cause kidney stones and acute renal failure if ingested in large amounts. According to the FDA, U.S. formula makers do not obtain ingredients for their products from China. But as reported in November, the agency had detected "trace" amounts of melamine in one sample of U.S. made infant formula. The Associated Press is reporting that the FDA says it has detected the chemicals in four of 89 containers of infant formula made in the United States. The new count comes from the same round of tests that led to the November Associated Press report, and represents an update, the agency said. According to the Associated Press, the updated results show that two additional containers of Enfamil LIPIL with Iron had traces of cyanuric acid.
Source: http://www.newsinferno.com/archives/4504

[Return to top]

Water Sector

14. *January 9, Associated Press* – (National) **EPA reconsiders regulating fuel in drinking water.** The U.S. Environmental Protection Agency (EPA) is reconsidering whether to limit the amount of a toxic rocket fuel ingredient allowed in drinking water. Earlier this year the agency proposed not setting a drinking water standard for perchlorate. The chemical has been detected at almost 400 sites in 35 states at levels high enough to interfere with thyroid function and pose developmental problems in humans. The agency on Thursday said it would not make a final decision until the National Academy of Sciences studies the matter. The EPA's own advisers and an inspector general report faulted EPA for how it evaluated the risk the chemical poses to human health. Perchlorate occurs naturally, but most contamination stems from defense and aerospace activities.
    Source: http://www.google.com/hostednews/ap/article/ALeqM5hSojurZeXMyhy1LDIz4uEPqvZr6wD95J54I01

15. *January 9, Associated Press* – (South Carolina) **Columbia: Sewage spill didn't contaminate water.** A 500,000 gallon sewage spill earlier last week did not contaminate drinking water in Columbia. The State newspaper reported on Friday that a city official said pollution levels in the canal where the drinking water is drawn showed no impact from Monday's spill on the Broad River. One of the city's drinking water plants is about a mile downstream from the spill site. The other is at Lake Murray. Drinking water is always treated to remove pollution. The Waterworks superintendent said additional tests were performed in the river and the canal and there was no increase in pollution. Officials say pumps that push the sewage through the pipe system failed. Some of the debris included bedding and a uniform from the Corrections Department. The prison system will install new screens to capture debris.
    Source: http://www.goupstate.com/article/20090109/ARTICLES/901090299/-1/SHRINEBOWL?Title=Columbia__Sewage_spill_didn_t_contaminate_water_

16. *January 8, Water Technology Online* – (Washington) **WA floods impacting treatment plants.** The mayor of Tacoma, Washington, has declared a civil emergency for the city of about 200,000 due to the threat the rising Puyallup River poses to the city's wastewater treatment plant, according to local reports. Tacoma, as well as most of northwestern Washington, has been inundated with floodwaters as snowmelt and rain swell rivers and caused mudslides and avalanches. The city of Spokane's wastewater treatment plant was processing about 70 million gallons a day, more than the average flow, the operator in charge told KXLY 4. The water, which is accompanied by higher-than-usual levels of sand, is now being treated with an abbreviated treatment process to get the water in and out faster. "When they are full we don't have any more storage capacity, then we have to process it, disinfect it and send it to the river," the operator is quoted as saying. In Orting, residents were helping to pack sandbags around the city's water treatment plant, the Associated Press reported on January 8.
    Source: http://www.watertechonline.com/news.asp?N_ID=71215

17. *January 8, WHO 13 Des Moines* – (Iowa) **Flushing of water system halts while more water is processed.** Thousands of southwest Iowa residents are still without safe drinking water after a filtration problem at the Creston Water Works two weeks ago. The problem has been fixed, but the flushing of the extensive system has now been halted because of a water supply issue. A boil order was put into place for customers of the Southern Iowa Rural Water Association. That affected 40,000 residents in seven Iowa counties. Tuesday, the order was lifted for residents of Creston only, after water from the Creston Water Works passed DNR testing. The boil order remains in effect for all other communities until the flushing process is completed, but now that process has halted because the Creston Water Works has been unable to keep up with the amount of water required for the flushing. Once an adequate amount of water can be processed, the flushing will continue. Thursday morning Creston Water Works discovered a leak in their system, but it has since been repaired and they continue to replenish the water supply in their towers.
    Source: http://www.msnbc.msn.com/id/28560846/

18. *January 8, Beacon Journal* – (Ohio) **Hartville mayor opposing sewer work.** The mayor of Hartville is opposing the proposed sewage plant expansion supported by Village Council and the Ohio Environmental Protection Agency (EPA). He told the council Tuesday that he does not favor commissioning design work, which is expected to cost $1 million. “Once we start that design, we are starting a design for a $6.4 million sewer plant,” he said. “It needs to be done,” said the chairman of the council’s sewer rate committee. “If the microstrainers go out, we’re out of business; we’re putting raw sewage into the creek,” he said. The Ohio EPA is willing to lend the village up to $6.2 million because the plant is operating close to its capacity, he said.
    Source: http://www.ohio.com/news/37254229.html

19. *January 7, Saginaw News* – (Michigan) **Saginaw River wastewater overflow within acceptable limits.** Hundreds of millions of gallons of potentially contaminated wastewater was discharged into the Saginaw River early last week, when treatment plants were overloaded with stormwater and sewage. Subsequent tests indicate the release was benign and the contaminates were below state Department of Public Health maximum limits. Overflows like this occur four or five times per year, said the City of Saginaw Wastewater Treatment Plant superintendent. The Saginaw County Department of Public Health environmental services director said overflows are normal when the area gets about 1 inch of rain, though the number of gallons discharged during this incident was high.
    Source:
    http://www.mlive.com/news/saginaw/index.ssf/2009/01/saginaw_river_wastewater_overf.html

[Return to top]

Public Health and Healthcare Sector

20. *January 8, WebMD* – (National) **Flawed results on some vitamin D tests.** Quest Diagnostics, a company that performs lab tests for patients nationwide, says some of the

vitamin D tests it conducted in 2007 and part of 2008 yielded incorrect results. Quest Diagnostics has already sent letters to the doctors of the patients with suspicious results on their vitamin D test, according to the medical director of the endocrinology lab at Quest Diagnostics Nichols Institute in San Juan Capistrano, California. The incorrect vitamin D tests tended to overestimate patients' blood levels of vitamin D. The errors stemmed from problems with the test's reagents and calibrators, and there were also "issues with some sites not following proper operating procedure."
Source: http://www.webmd.com/news/20090108/flawed-results-on-some-vitamin-d-tests

21. *January 8, HealthDay News* – (National) **Common flu strain resistant to popular antiviral drug.** The most common strain of flu this season is resistant to the popular antiviral drug Tamiflu, but government health officials said Thursday there is no reason to panic. The fact that the flu season so far has been slow, and that other drugs work well against this particular flu virus, has health officials adopting a watchful attitude for now. While the cause of the mutation that made the virus resistant to Tamiflu (oseltamivir) is not known, experts suspect it was caused by the wide use of Tamiflu in other countries to treat upper respiratory infections. There were reports last year from Europe and other countries that a certain type of flu (H1N1) was resistant to oseltamivir, according to the chief of flu prevention at the U.S. Centers for Disease Control and Prevention.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2009/01/08/AR2009010803411.html

[Return to top]

Government Facilities Sector

22. *January 8, Joplin Globe* – (Kansas) **Bomb threat at courthouse investigated.** The Cherokee County Courthouse was evacuated January 7 after the sixth bomb threat since 2005. The Columbus police chief said a caller to a dispatcher at the Cherokee County Sheriff's Department, which is not housed in the courthouse, said there was a bomb in the courthouse. The call came in about 2 p.m. The courthouse was evacuated, and the courthouse square was closed to traffic. The courthouse was closed for the rest of the day January 7. The Kansas Highway Patrol was transporting bomb-sniffing dogs from Topeka to go through the building to determine if any explosives were present. After the most recent bomb threat, which came on Sept. 29, a protocol was presented for employees to follow when a bomb threat is phoned in to the courthouse. The protocol included training employees to use a feature called customer-originated trace. It was not clear January 7 whether the Sheriff's Department was able to trace the call.
Source: http://www.joplinglobe.com/neo_sek/local_story_008003630.html

23. *January 8, Greensboro News-Record* – (North Carolina) **Suspicious package at courthouse isn't hazardous.** A suspicious envelope found Thursday at the federal courthouse downtown brought the city's hazardous materials team to the building. The envelope was deemed suspicious based on how it was packaged, according to police. Security guards at the courthouse X-rayed the envelope and determined that it did not

contain explosives. Police and fire officials were called shortly before 10 a.m. "Coming to a federal building, we want to cover all our bases," said a lieutenant of the Greensboro Police Department. The courthouse was not evacuated. About 10:45 a.m., authorities determined the envelope contained a letter.
Source: http://www.news-record.com/content/2009/01/08/article/suspicious_package_found_at_federal_courthosue

[Return to top]

Emergency Services Sector

24. *January 9, NewsDay* – (New York) **Cops look to jam cell phones if terror strikes.** The NYPD is examining ways to shut down cell phone calls in and around future hostage-taking scenarios without also shutting down the communications devices of the police trying to rescue them, the police commissioner said at a congressional hearing Thursday. Cell phones were simple tools used to deadly effect in the Mumbai terror attacks, he told the Senate Homeland Security and Governmental Affairs. According to phone transcripts, the attackers received instructions and real-time updates about the officers amassing against them. Some of the phones they used for the calls apparently were taken from hostages. That information, investigators believe, helped make the attack much more deadly as the gunman delayed capture.
Source: http://www.newsday.com/services/newspaper/printedition/friday/news/ny-nycell095992155jan09,0,836875.story

[Return to top]

Information Technology

25. *January 9, Register* – (International) **HP hunts down 'rare' BladeSystem problem.** A power supply failure in HP BladeSystem c7000 enclosures can cause the whole BladeSystem to fail, the firm has admitted. According to an HP advisory note: "HP has identified a potential, yet extremely rare issue with HP BladeSystem c7000 Enclosure 2250W Hot-Plug Power Supplies manufactured prior to March 20, 2008. "This issue is extremely rare; however, if it does occur, the power supply may fail and this may result in the unplanned shutdown of the enclosure, despite redundancy, and the enclosure may become inoperable." So, the issue is extremely rare, says HP. But it applies to any HP BladeSystem c7000 Enclosure configured with an HP c7000 Power Supply, if the power supply was manufactured before March 20, 2008. Each enclosure can have up to a total of six supplies.
Source: http://www.theregister.co.uk/2009/01/09/hp_bladesystem_problem/

26. *January 9, DarkReading* – (International) **Slow and silent targeted attacks on the rise.** The most determined cybercriminals do not necessarily work fast when they breach a network, and their infiltration is often silent and undetectable. But it is this brand of "low and slow" targeted attack that can also be the most deadly, security experts say. This is a methodical attack, where the attacker covers his tracks as he penetrates the

network, sometimes ceasing the attack for days at a time to avoid raising suspicion. It is typically a nearly invisible hack that is not discovered until it is too late, after the bad guys have made off with valuable data and done serious damage. Security experts say IT and security managers need to be at the ready for these highly targeted attacks, which may be more common than once thought. No one knows for sure just how widespread these attacks are today, but some basic characteristics are present as to how they are executed. The attacker typically initially gains access through a Web application vulnerability, or via a successful spear-phishing attack on an employee. After he gets inside, he may wait a few days or so after this first stage of the attack.
Source:
http://www.darkreading.com/security/attacks/showArticle.jhtml;jsessionid=0NURT4VR50P3YQSNDLPSKHSCJUNN2JVN?articleID=212701434

27. *January 8, CNET News* – (International) **Fake CNN site from phishing e-mail hides a Trojan.** A new e-mail that is circulating looks like it comes from CNN and links to a fake CNN Web page offering "graphic" video related to the Israel-Hamas conflict but instead hosts a Trojan that steals sensitive data, RSA said on January 8. When someone clicks on the video link on the fake CNN site an error message pops up urging the visitor to download the latest version of Adobe Flash Player. Clicking on the download link installs a "SSL stealer" Trojan that captures financial and other sensitive information, RSA said in a blog. The Trojan looks for encrypted communications between the computer and known financial institutions and when it sees data being sent it diverts it to a malicious third-party, said the vice president of product management and strategy at RSA.
Source: http://news.cnet.com/8301-1009_3-10137863-83.html?tag=newsEditorsPicksArea.0

28. *January 8, CNET News* – (International) **Latest problem import? Infected digital photo frames.** Digital photo frames infected with computer viruses are the latest problem import from China. "Essentially, it's a supply chain problem," said the director of the Internet Storm Center at the SANS Institute. The culprit is believed to be poor quality-assurance testing procedures in which one of every 1,000 or so devices is plucked off an assembly line and tested on a computer that is infected with a virus, he said. Before Christmas, Samsung and Amazon issued alerts warning customers that some Photo Frame Driver CDs for Samsung's SPF line of digital photo frames contained a virus in the frame manager software. Customer PCs running Windows XP are at risk of being infected by the virus, W32.Sality.AE, which drops a keylogger or backdoor onto the system. Element and Mercury brand frames sold at Circuit City and Wal-Mart, respectively, also were reported to be infected, according to the San Francisco Chronicle. "Anything that has flash storage or bootable storage is exposed to this kind of threat," said the director of security research for McAfee Avert Labs. "It doesn't mean you shouldn't buy them. You should just realize before you plug it in that you might want to disable the Windows auto-boot functionality and run an antivirus scan on it, just to be safe."
Source: http://news.cnet.com/8301-1009_3-10137032-83.html?part=rss&tag=feed&subj=News-Security

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

29. *January 8, RCR Wireless News* – (District of Columbia) **DC cell phone jamming demo canceled.** The District of Columbia cancelled Thursday's scheduled cell phone jamming demonstration at a city jail. Cellular industry association CTIA Wednesday petitioned a federal appeals court to overturn the Federal Communication Commission's (FCC) January 2 order permitting the District of Columbia Department of Corrections to host a demonstration using equipment supplied by CellAntenna Corp. The FCC told the court the cell phone jamming event had been cancelled by the District of Columbia Department of Corrections and was not rescheduled. Given the events, CTIA withdrew its appeals court petition. The District of Columbia Department of Corrections director requested permission for the jamming demonstration in a December 16 letter to the outgoing FCC chairman. He wrote that the proliferation of contraband cell phones has become a major security risk within corrections facilities around the country and that handsets are being used by prisoners to intimidate witnesses, coordinate escapes, and conduct criminal enterprises. Wireless providers appear worried that any policy changes could lead to a proliferation of cell phone jammers that citizens could use to halt annoying cell phone conversations at restaurants, movies, and other public venues. Federal law forbids citizens as well as state and local law enforcement from using cell phone jammers, while U.S. agencies are not bound by the prohibition.
Source: http://www.rcrwireless.com/article/20090108/WIRELESS/901089987/1082/dc-cellphone-jamming-demo-canceled

[Return to top]

Commercial Facilities Sector

30. *January 9, KPIX 5 San Francisco, Associated Press, and BCN* — (California) **2nd night of violent BART protests in Oakland.** About 100 protesters were back on the streets Thursday night in Oakland, protesting the fatal shooting of a 22-year-old, unarmed man by a Bay Area Rapid Transit (BART) police officer. The unruly protesters smashed store windows, burned cars, and vandalized an Oakland police cruiser as they made their way throughout the downtown area. Police in riot gear shut down a main thoroughfare in Oakland after protesters tried to stop cars and threw trash cans into the street. An organizer of the protest said a group of anarchists not associated with the organizations hosting the rally had smashed a police vehicle before setting a garbage can on fire — triggering the rioting. The protests were calmer than the previous night when at least 120

people were arrested following a violent rampage that damaged about 300 businesses and numerous cars. Charges against those arrested include inciting a riot, assault on a police officer, vandalism, rioting, and unlawful assembly, an Oakland Police spokesman said. Two of the arrests involved illegal handgun possession. He indicated at least one person, a TV cameraman, was injured in the violence. No police officers were hurt, he said.
Source: http://cbs5.com/local/BART.shooting.protest.2.902981.html

31. *January 8, Associated Press* – (Minnesota) **RNC protestor pleads guilty.** One of two Texas men accused of possessing Molotov cocktails during the Republican National Convention has pleaded guilty. The U.S. Attorney's Office says the Austin man pleaded guilty Thursday in federal court in Minneapolis to one count of aiding and abetting possession of an unregistered firearm. A sentencing date has not been set. Meanwhile his co-defendant, also of Austin, is scheduled to go on trial on January 26. Prosecutors allege the pair were part of an Austin-based protest group that planned to use incendiary devices to destroy property or injure police during the Republican National Convention. The convention was at the Xcel Energy Center in St. Paul, September 1-4.
Source: http://www.huffingtonpost.com/2009/01/08/rnc-protester-pleads-guil_n_156340.html?view=print

[Return to top]

National Monuments & Icons Sector

32. *January 9, State Island Advance* – (New York) **Radioactive soil removed from Great Kills Park.** National Park Service officials are removing what they describe as "a small amount of soil" containing traces of radioactive material from Great Kills Park in New York. The work, which was expected to be completed by January 9, includes five sites where a total of one cubic yard of soil will be removed for disposal. Officials say the hot spots are safe by federal standards and are not in high visitor-use areas. The source of radiation was probably from remnants of old industrial machinery that was dumped in the park in the 1930s, officials speculated. The project is being done in conjunction with the U.S. Army Corps of Engineers, the state Department of Environmental Conservation, and the U.S. Environmental Protection Agency.
Source: http://www.silive.com/news/advance/index.ssf?/base/news/12315087299430.xml&coll=1

33. *January 8, OregonLive.com* – (Washington) **Washington forests hard hit by storm.** Washington's Mount Baker/Snoqualmie National Forest sent out a warning about travel in the Washington Cascades and Olympics, stating: Winter sports enthusiasts should check conditions in advance of their visits to ski, snowshoe, and snowmobile. Many state highways and county roads accessing the national forests are closed. As floods, avalanches, and landslides threaten roads throughout the state, visitors to National Forests are advised to use caution. Some forest roads that were not closed because of snow pack now may be impassable because of downed trees, or road and bridge washouts. The extent of the damage on the national forests may not become evident

until the snow thaws.
Source:
http://blog.oregonlive.com/terryrichard/2009/01/washington_forests_hard_hit_by.html

[Return to top]

Dams Sector

34. *January 9, Associated Press* – (Alabama) **TVA waste pond ruptures in Ala.; spill contained.** A waste pond at a coal-burning power plant in northeast Alabama ruptured Friday, but the spill was quickly contained, utility officials said. It was the second breach at a Tennessee Valley Authority (TVA) facility in less than a month. The leak was discovered at about 6 a.m. Friday at the plant near Stevenson, said a TVA spokesman. Most of the material from the leak flowed into a settling pond at the plant site, but some spilled into nearby Widows Creek, he said. The leak had stopped by late morning and TVA was conducting temporary repairs on the pond, he said. State emergency management officials are trying to determine if any drinking water systems might be affected by the spill into the creek, which flows into the Tennessee River, said a spokesman for the Alabama Department of Environmental Management.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5jUmVbOILCk2YLsx92cubV-aN1c_QD95JP8PO0

35. *January 9, Knoxville News Sentinel* – (Tennessee) **TVA dam work spills Ocoee River bottom sediment.** An Ocoee rafting company owner says he is not concerned about any bottom soil accidentally spilled into the Ocoee River from work being done on a river dam. The Ocoee Adventure Center owner said he had not heard about the spill when contacted on Friday, but recent rains sent more than 10,000 cubic feet per second of water rushing down the Ocoee, and any silt is probably in Parksville Lake. The Tennessee Valley Authority (TVA) discovered on Sunday that silt had spilled into the river from the No. 3 dam after water was held back while workers did repair work on the No. 2 dam downstream. The TVA spokesman said when the water was released after the work was completed, some bottom silt spilled into the river at a site above the Ocoee Whitewater Center. The No. 3 dam has a large amount of silt in the lake due to years of erosion from the copper mining area of the Copper Basin. A TVA official had said that the repairs to the dam required sluicing water downstream to lower water for workers' safety. That process pulled sediment through a sluice gate down the river.
Source: http://www.knoxnews.com/news/2009/jan/09/tva-dam-work-spills-ocoee-river/

36. *January 9, New Orleans Times-Picayune* – (Louisiana) **Corps study to analyze levees, coast.** The Army Corps of Engineers will study the feasibility of both building levees and undertaking coastal restoration projects in southwestern Louisiana, to protect populated areas in Vermilion, Calcasieu, and Cameron parishes while improving natural habitats for wildlife, Corps and state officials announced Thursday. The tactic sets a promising precedent for all levee projects in that it seeks to create one strategy combining coastal restoration and levee-building — projects that often conflict with one another. A reconnaissance study completed in 2007 recommended that this new

investigation focus on three major levee alternatives, but the state and the Corps agreed to broaden the focus to include both levee and restoration alternatives, said the director of the state Office of Coastal Protection and Restoration. The study still will include an investigation into the feasibility of building a controversial $2.1 billion, 120-mile-long, 12-foot-high armored earthen levee. The levee project would run along the southern bank of the Gulf Intracoastal Waterway through the three parishes. Such a levee would dramatically reduce flooding from surge caused by a hurricane with a 1 percent chance of occurring in any year — a so-called 100-year storm — which is the same standard being used for levee improvements in the New Orleans area. The study also will consider two short, U-shaped non-armored earthen levee alternatives that would protect the city of Lake Charles and most populated sections of Vermilion Parish from 100-year events. Those two alternatives would cost $607 million and $572 million, respectively. The new study also will include alternatives for rebuilding the complicated Chenier Plain, a series of forested, east-west ridges that are at most just 10 feet high, separated by stretches of wetlands. It will build on past studies of the unique coastal formation in that part of the state, as well as a variety of new scientific studies completed in the aftermath of last year's hurricanes, said a state coastal protection official. Creation of new barrier islands and coastal marsh areas and protecting smaller communities with ring levees will be studied.
Source: http://www.nola.com/news/t-p/index.ssf?/base/news-1/12314820359580.xml&coll=1

37. *January 8, HeraldNet* – (Washington) **Levees breached in Stanwood, Snohomish.** Fire crews in Stanwood were forced to abandon their efforts to shore up an area along 2500 block 95th Avenue NW as flood waters began to rise and threaten their only way out. Crews and high school students spent the morning sandbagging to keep the water from spilling over Highway 532 and flooding a residential area south of city. Fire crews retreated when water began to creep up along 98th Avenue NW, said a battalion chief with North County Fire and EMS. Meanwhile, Snohomish city officials reported about 1 p.m. that a levee along the Pilchuck River breached, causing evacuations of homes nearby on Sixth Street, said the city manager. No one was hurt. Thursday morning, water was flowing over the top of the levee at French Creek. First Street west of Avenue D in downtown Snohomish was shut down Thursday morning as officials brace for what could be the worst flood on record. Even the revised prediction has the river topping levees and inundating much of the river valley. The Snohomish River likely will take a long time returning to its banks because anticipated high tides will act like a dam on the lower river. The Stillaguamish River at Arlington crested at 10 a.m. Thursday at 20.8 feet. A breach in a dike there flooded farmland and shut down businesses on the east side of Island Crossing. On Thursday, floodwaters blew a hole in the Ebey Island Slough Dike just before 8 p.m., and Snohomish County emergency officials urged residents of the island to try to leave as soon as possible. The breach measures 20 feet by 5 feet, and is located east of the Snohomish River, about half a mile south of Highway 2.
Source: http://www.heraldnet.com/article/20090108/NEWS01/901089973/0/SPORTS
See also: http://www.heraldnet.com/article/20090108/NEWS01/901089919

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.
To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer